Amendments to the Specification:

Please replace the paragraph starting on page 5, line 6 with the following amended paragraph:

From Fig. 1 and the above description, it is evident that at least four data bus operations are necessary for each packet. Since data busses often form a bottleneck in system performance, the resulting system is often inefficient. Even though[[,]] all processing of encryption and data integrity is performed by a special processor 8, the resulting improvement in system performance is not substantial.

Please replace the paragraph starting on page 8, line 21 with the following amended paragraph:

The ciphering system in the form of an ASIC or an FPGA includes means to look up the security association determined by the host processor. The security association is, for example, a ~~the~~ security context in which a packet is to be ciphered including keys and ciphering algorithms. The host processor includes means for determining a security association and for storing the determined security association in a location accessible by the ciphering processor. For example, the security association is stored in the dual ported RAM. Alternatively, the security association is stored in memory within the ciphering processor.

Please replace the paragraphs beginning on page 3, line 20 to the end of the last paragraph before the heading "Brief Description of the Drawings" at page 4, line 7 of the original specification with the following amended paragraphs:

In the first aspect, a system for ciphering a packet in a data stream received by a communication device is provided. The system includes a memory device having a memory buffer, a first access port connected to the memory buffer and a second access port connected to the memory buffer. The system includes a first communication port for receiving the data stream and a second communication port for transmitting a ciphered data stream associated with the data stream. The system also has a data processing processor connected to the communication ports and the first access port via a first bus

and a ciphering processor connected to the second access port via a second bus. The first access port and the second access port each provide access to the memory buffer. The data processing processor is adapted to receive the data stream and provide it to the memory buffer over the first bus, to identify a start and an end of the packet, to store a file associated with the packet in the memory buffer through the first bus and to retrieve the ciphered data stream from the memory buffer through the first bus for transmission through the second communication port. The data processor includes a security module to determine a security context relating to at least one source of the data stream and a destination for the ciphered data stream, to store the security context in the memory buffer for access by the ciphering processor and to retrieve a given security context from the memory buffer for use in generating the ciphered data stream. The ciphering processor is adapted to retrieve the file from the memory buffer over the second bus, generate the ciphered data stream from the file, generate integrity check information for the ciphered data stream using the file and provide the ciphered data stream to the memory buffer over the second bus.

The ciphering processor may include an encryption module for generating the ciphered data and a module for generating the integrity check information. The module may be a hashing module.

The encryption module may include a DES encryption module for performing one of DES and triple-DES encryption.

The module may include a HMAC hashing module for encoding the integrity check information within the ciphered data.

The memory buffer may include dual port random access memory.

~~The data processing processor may include a security module. The security module may retrieve a security context from memory. The security context may be used in generating the ciphered data stream.~~

~~The security module may determine a security context relating a source of the data or a destination for the ciphered data stream and may store the security context in the~~

~~memory buffer. The security context stored may be accessible by the ciphering processor.~~

The data processing processor may include a security address module. The security address module may store an address associated with the security context in the memory buffer. The address may be based on the source of the data or the destination for the ciphered data.

The security module may provide an indication to the data processing processor when a security context is not present in the memory buffer.

The data processing processor may operate asynchronously to the ciphering processor.

The data processing processor may be clocked by a first clock source and the ciphering processor may be clocked by a second clock source. The first clock source may be asynchronous to the second clock source.

The data received at the first communications port may include fragments of a packet. The data processing processor may store the fragments in the memory buffer to assemble the packet. The ciphering processor may generate the ciphered data stream from the assembled packet.

The system may be disposed at a gateway between a private network and a public network in a secure virtual private network. The first communications port may be connected to the private network or the public network and the second communications port may be connected to the other one of the private network and the public network.

In a second aspect, a method for ciphering a packet in a data stream received by a communication device is provided. The device has a first communication port for receiving the data stream, a second communication port for transmitting a ciphered data stream associated with the data stream, a memory device, a data processing processor connected to the first and second communication ports and the access port via a first bus and a ciphering processor connected to the second access port via a second bus. The

memory device includes a memory buffer and a first and a second access ports connected to the memory buffer. The method comprises receiving the data stream from the first communication port for processing by the data processing processor; identifying a start and an end of the packet by the data processing processor; storing a file associated with the packet in the memory buffer by the data processing processor through the first bus; retrieving the file from the memory buffer by the ciphering processor over the second bus; generating the ciphered data stream from the file by the ciphering processor; generating integrity check information for the ciphered data stream using contents of the file by the ciphering processor; ~~and~~ providing the ciphered data stream to the second communication port; retrieving a security context from memory for use in generating the ciphered data stream; determining a security context relating to at least one of a source of the data stream and a destination for the ciphered data stream; and storing the security context in the memory buffer. The stored security context is accessible by the ciphering processor.

The ~~method may further retrieve a security context from memory for use in generating the~~ ciphered data stream may be generated by an encryption module in the ciphering processor and the integrity check information may be generated by a hashing module in the ciphering processor. ~~; determine a security context relating to at least one of a source of the data stream and a destination for the ciphered data stream; and store the security context in the memory buffer, the security context stored being accessible by the ciphering processor.~~

The ciphering processor may include an encryption module for generating the ciphered data stream and a module for generating the integrity check information.

The encryption module may perform one of DES and triple-DES encryption utilizing a DES encryption module.

The hashing module may encode the integrity check information within the ciphered data stream utlizing a HMAC hashing module.

The memory buffer may comprise dual port random access memory.

The data processing processor may store an address associated with the security context in the memory buffer. The address may be based on at least one of the source of the data stream and the destination for the ciphered data stream.

The security module may provide an indication to the data processing processor when a security context is not present in the memory buffer.

The data processing processor may be clocked by a first clock source, the ciphering processor may be clocked by a second clock source and the first clock source may be asynchronous to the second clock source.

In a third aspect, a system for ciphering packet in a data stream received by a communication device is provided. The system includes a first communication port for receiving the data stream; a second communication port for transmitting a ciphered data stream associated with the data stream; and a memory having a memory buffer, a first access port connected to the memory buffer, and a second access port connected to the memory buffer. The system includes a data processing processor connected to the first communication port, the second communication port and the first access port via a first bus. The data processor includes a security module to determine a security context relating to at least one source of data stream and a destination for the ciphered data stream, to store the security context in the memory buffer for access by the ciphering processor and to retrieve a given security context from the memory buffer for use in generating the ciphered data stream. The system includes a ciphering processor connected to the second access port via a second bus. The first access port and second access port each provide access to the memory buffer, and the ciphering processor provides the ciphered data stream to the memory buffer through the second bus.

* * * * *